AMENDMENTS TO THE CLAIMS

Upon entry of this amendment, the following listing of claims will replace all prior versions and listings of claims in the pending application.

IN THE CLAIMS

Please amend claims 1, 16 and 21, and add claims 26-39 as follows:

1. (Currently Amended) A method for enabling strong mutual authentication on a computer network comprising the steps of:

transmitting, by a first computer, a first encrypted message to a second computer over a first communication channel, said first encrypted message comprising a first authentication number encrypted with a second authentication number;

receiving, by said second computer, a second message over a second communication channel, wherein said second message comprises ~~a~~ said second authentication number used to decrypt said first encrypted message ~~and~~;

receiving, by said first computer, from said second computer a third encrypted message over said first communication channel, said third encrypted message comprising said second authentication number encrypted with said first authentication number; and

determining, by said first computer, said second authentication number of said third encrypted message is the same as said second authentication number used to encrypt said first encrypted message.

2. (Previously Presented) The method of claim 1, authenticating, by said first computer, the second computer in response to said determination.

3. (Previously Presented) The method of claim 1, comprising decrypting, by said second computer, said first encrypted message using said second authentication number of the second message

4. (Original) The method of claim 1 further comprising transmitting a first indicia to said first computer over said first communication channel.

5. (Previously Presented) The method of claim 2 further comprising generating, by said first computer, at least one of said first authentication number or said second authentication number.

6. (Original) The method of claim 1 further comprising generating, by said first computer, a third authentication number.

7. (Previously Presented) The method of claim 1 further comprising transmitting, by said first computer, said second message to a verifier over said a third communication channel and transmitting by said verifier said second message to said second computer over said second communication channel, wherein said second message comprises said second authentication number encrypted.

8. (Previously Presented) The method of claim 1, comprising generating, by said second computer, said third encrypted message by encrypting said second authentication number of said second message with said first authentication number of said first encrypted message from said first computer.

9. (Original) The method of claim 1, wherein said second message further comprises a third authentication number.

10. (Original) The method of claim 7 further comprising decrypting, by said verifier, said second message to obtain a first decrypted message, wherein said first decrypted message comprises said second authentication number.

11. (Previously Presented) The method of claim 7, wherein said verifier comprises one of a third computer, a mobile communications device or a subscriber identification module.

12. (Previously Presented) The method of claim 2 further comprising decrypting, by said second computer, said first message transmitted by said first computer to recover said first authentication number.

13. (Original) The method of claim 1 further comprising transmitting, by said second computer, a third message to said first computer over said first communication channel, wherein said third message comprises said second authentication number encrypted by said first authentication number.

14. (Previously Presented) The method of claim 13 further comprising validating said second computer by said first computer by decrypting said third message to obtain said second authentication number.

15. (Original) The method of claim 1, wherein said second message further comprises an encrypted portion.

16. (Currently Amended) A system for enabling strong mutual authentication comprising:

a first computer transmitting a first encrypted message over a first communication channel, said first encrypted message comprising a first authentication number encrypted with a second authentication number;

a second computer receiving said first encrypted message over said first communication channel and said second computer receiving a second message over a second communication channel, said second message comprising said ~~a~~ second authentication number used to decrypt said first encrypted message; and

wherein said first computer, receives from said second computer over said first communication channel a third encrypted message comprising said second authentication number encrypted with said first authentication number, and determines said second authentication number of said third encrypted message is the same as said second authentication number used to encrypt said first encrypted message.

17. (Previously Presented) The system of claim 16 wherein said first computer authenticates said second computer in response to said determination.

18. (Previously Presented) The system of claim 16 wherein said second computer decrypts said first encrypted message using said second authentication number of the second message.

19. (Previously Presented) The system of claim 16, wherein a verifier transmits said second message to said second computer over said second communication channel, said verifier comprising one of a third computer, a mobile communications device or a subscriber identification module.

20. (Previously Presented) The system of claim 19 wherein said first computer transmits to said verifier said second message encrypted and said verifier decrypts said encrypted second message to obtain a key to decrypt said first encrypted message.

21. (Currently Amended) An apparatus for enabling strong mutual authentication on a computer network comprising:

means for transmitting, by a first computer, a first encrypted message to a second computer over a first communication channel, said first encrypted message comprising a first authentication number encrypted with a second authentication number;

means for receiving, by said second computer, a second message over a second communication channel, wherein said second message comprises ~~a~~ said second authentication number used to decrypt said first encrypted message;

means for receiving, by said first computer, from said second computer a third encrypted message over said first communication channel, said third encrypted message comprising said second authentication number encrypted with said first authentication number; and

means for determining, by said first computer, said second authentication number of said third encrypted message is the same as the second authentication number used to encrypt said first encrypted message.

22. (Canceled).

23. (Canceled).

24. (Original) The method of claim 1, comprising determining, by said first computer, said second authentication number of said third encrypted message is not the same as said second authentication number used to encrypt said first encrypted message.

25. (Original) The method of claim 24, comprising not authenticating, by said first computer, said second computer in response to said determination.

26. (New) The apparatus of claim 21, comprising means for authenticating, by said first computer, the second computer in response to said determination.

27. (New) The apparatus of claim 21, comprising means for decrypting, by said second computer, said first encrypted message using said second authentication number of the second message

28. (New) The apparatus of claim 21, comprising means for transmitting a first indicia to said first computer over said first communication channel.

29. (New) The apparatus of claim 26, comprising means for generating, by said first computer, at least one of said first authentication number or said second authentication number.

30. (New) The apparatus of claim 21, comprising means for generating, by said first computer, a third authentication number.

31. (New) The apparatus of claim 21, comprising means for transmitting, by said first computer, said second message to a verifier over said a third communication channel and transmitting by said verifier said second message to said second computer over said second communication channel, wherein said second message comprises said second authentication number encrypted.

32. (New) The apparatus of claim 21, comprising means for generating, by said second computer, said third encrypted message by encrypting said second authentication number of said second message with said first authentication number of said first encrypted message from said first computer.

33 (New) The apparatus of claim 21, wherein said second message further comprises a third authentication number.

34. (New) The apparatus of claim 31, comprising means for decrypting, by said verifier, said second message to obtain a first decrypted message, wherein said first decrypted message comprises said second authentication number.

35. (New) The apparatus of claim 31, wherein said verifier comprises one of a third computer, a mobile communications device or a subscriber identification module.

36. (New) The apparatus of claim 26, comprising means for decrypting, by said second computer, said first message transmitted by said first computer to recover said first authentication number.

37. (New) The apparatus of claim 21, comprising means for transmitting, by said second computer, a third message to said first computer over said first communication channel, wherein said third message comprises said second authentication number encrypted by said first authentication number.

38. (New) The apparatus of claim 37, comprising means for validating said second computer by said first computer by decrypting said third message to obtain said second authentication number.

39. (New) The apparatus of claim 21, wherein said second message further comprises an encrypted portion.